

# Exhibit A

[Click here to Respond to Selected Documents](#)

Sort Date Entries: Descending Ascending

Display Options: All Entries ▼

05/29/2025

**Corporation Served**

Document ID - 25-SMCC-8266; Served To - AMERICAN MULTISPECIALTY GROUP, INC.; Served Date - 05/23/2025; Served Time - 13:50:01; Service Type - SP; Reason Description - SERV; Service Text -

**Notice of Service**

Return of Service.

**Filed By:** JOHN FRANCIS GARVEY JR

**On Behalf Of:** MICHAEL GARSIDE

05/20/2025

**Summons Issued-Circuit**

Document ID: 25-SMCC-8266, for AMERICAN MULTISPECIALTY GROUP, INC. Summons Attached in PDF Form for Attorney to Retrieve from Secure Case.Net and Process for Service.

05/19/2025

**Filing Info Sheet eFiling**

**Filed By:** JOHN FRANCIS GARVEY JR

**Motion Special Process Server**

Request for Appointment of Special Process Server.

**Filed By:** JOHN FRANCIS GARVEY JR

**On Behalf Of:** MICHAEL GARSIDE

**Pet Filed in Circuit Ct**

Class Action Complaint.

**Filed By:** JOHN FRANCIS GARVEY JR

**On Behalf Of:** MICHAEL GARSIDE

**Judge Assigned**

DIV 15

IN THE CIRCUIT COURT OF SAINT LOUIS COUNTY  
STATE OF MISSOURI

**MICHAEL GARSIDE**, on behalf of himself  
and all others similarly situated,

Plaintiff,

v.

**AMERICAN MULTISPECIALTY GROUP,  
INC. d/b/a ESSE HEALTH,**

SERVE: 12655 Olive Blvd., Floor 4  
St. Louis, MO 63141

Defendant.

Case No.

**DEMAND FOR JURY TRIAL**

**CLASS ACTION COMPLAINT**

Michael Garside (“Plaintiff”), through his attorneys, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant American Multispecialty Group, Inc. d/b/a Esse Health (“Esse” or “Defendant”), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. Plaintiff alleges the following on information and belief—except as to his own actions, counsel’s investigations, and facts of public record.

**NATURE OF ACTION**

1. This class action arises from Defendant’s failure to protect highly sensitive data.
2. Esse is “the St. Louis area's largest independent physician's group” consisting of “100+ independent physicians and 45 offices.”<sup>1</sup>

---

<sup>1</sup> Esse Health Overview, LinkedIn, <https://www.linkedin.com/company/esse-health/about/> (last visited May 19, 2025).

3. As such, Defendant stores a litany of highly sensitive personal identifiable information (“PII”) and protected health information (“PHI”) (collectively “PII/PHI”) about its current and former patients. But Defendant lost control over that data when cybercriminals infiltrated its insufficiently protected computer systems in a data breach (the “Data Breach”).

4. Upon information and belief, the Data Breach impacted Defendant’s current and former patients.

5. In April 2025, Defendant posted a “Network Update” to its website explaining that its systems had to go offline due to a cybersecurity event.<sup>2</sup> In other words, Defendant had no effective means to prevent, detect, stop, or mitigate breaches of its systems—thereby allowing cybercriminals unrestricted access to its current and former patients’ PII/PHI.

6. On information and belief, cybercriminals were able to breach Defendant’s systems because Defendant failed to adequately train its employees on cybersecurity and failed to maintain reasonable security safeguards or protocols to protect the Class’s PII/PHI. In short, Defendant’s failures placed the Class’s PII/PHI in a vulnerable position—rendering them easy targets for cybercriminals.

7. Plaintiff is a Data Breach victim. He brings this class action on behalf of himself, and all others harmed by Defendant’s misconduct.

8. The exposure of one’s PII/PHI to cybercriminals is a bell that cannot be unrung. Before this data breach, its current and former patients’ private information was exactly that—private. Not anymore. Now, their private information is forever exposed and insecure.

---

<sup>2</sup> Network Update, Esse, <https://web.archive.org/web/20250507140756/https://www.essehealth.com/network-updates/> (last visited May 15, 2025).

## **PARTIES**

9. Plaintiff, Michael Garside, is a natural person and citizen of Missouri, where he intends to remain.

10. Defendant, American Multispecialty Group Inc, d/b/a Esse Health, is a Missouri for-profit business with its principal place of business at 12655 Olive Blvd Fl 4 Saint Louis, MO 63141-6386.

## **JURISDICTION AND VENUE**

11. This Court has subject matter jurisdiction pursuant to Mo. Stat. § 478.070.

12. This Court has personal jurisdiction because Defendant regularly conducts business in Missouri and because Plaintiff was injured while residing in Missouri.

13. Venue is proper in this Court under Mo. Rev. Stat. § 508.010 because Plaintiff's injuries occurred in Saint Louis County.

## **BACKGROUND**

### ***Defendant Collected and Stored the PII/PHI of Plaintiff and the Class***

14. Defendant is "one of the largest independent primary care groups in the Midwest" with 45 offices throughout the St. Louis area and more than 100 physicians and medical providers.<sup>3</sup>

15. As part of its business, Defendant receives and maintains the PII/PHI of thousands of its current and former patients.

16. In collecting and maintaining the PII/PHI, Defendant agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff and Class members themselves took reasonable steps to secure their PII/PHI.

---

<sup>3</sup> About Us, Esse, <https://www.essehealth.com/about-us/> (last visited May 19, 2025).

17. Under state and federal law, businesses like Defendant have duties to protect its current and former patients' PII/PHI and to notify them about breaches.

18. Defendant recognizes these duties, declaring in its "Privacy Policy" that:

- a. "Esse Health is committed to safeguarding the information Users entrust to Esse Health;" and
- b. "Information about Users that is maintained on Esse Health's systems is protected using industry standard security measures."<sup>4</sup>

19. Defendant further acknowledges its duties in its "Notice of Health Information Practices," stating that "Esse Health is required to: [p]rotect the privacy of your health information."<sup>5</sup>

20. Despite recognizing its duty to do so, on information and belief, Defendant has not implemented reasonably cybersecurity safeguards or policies to protect its patients' PII/PHI or supervised its IT or data security agents and employees to prevent, detect, and stop breaches of its systems. As a result, Defendant leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to patients' PII/PHI.

### ***Defendant's Data Breach***

21. In April 2025, Defendant announced that its systems were "offline due to a cybersecurity event."<sup>6</sup>

---

<sup>4</sup> Privacy Policy, Esse, <https://www.essehealth.com/privacy-policy/> (last visited May 19, 2025).

<sup>5</sup> Notice of Health Information Practices, Esse, <https://web.archive.org/web/20070709160523/http://essehealth.com/PDFs/NoticeofHealthInformationPractices.pdf> (last visited May 16, 2025).

<sup>6</sup> Network Update, Esse, <https://web.archive.org/web/20250507140756/https://www.essehealth.com/network-updates/> (last visited May 15, 2025).

22. Defendant's Data Breach resulted in the exposure of current and former patients' information and caused patients' appointments to be delayed and/or cancelled.

23. Due to the obfuscating nature of Defendant's Network Update, it is unclear how long cybercriminals had unfettered access to peruse and exfiltrate PII/PHI before being detected.

24. And yet, Defendant has still not begun sending formal notices to victims of the breach.

25. Thus, Defendant has kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

26. Defendant failed its duties when its inadequate security practices caused the Data Breach. In other words, Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII/PHI. And thus, Defendant caused widespread injury and monetary damages.

27. On information and belief, Defendant failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures.

28. It is unknown how many individuals were impacted by the Data Breach, however upon information and belief, the victims include Defendant's current and former patients.

29. Further, Defendant's "Network Update" shows that Defendant cannot—or will not—determine the full scope of the Data Breach, as Defendant has been unable to determine precisely when the cybercriminals gained access to its systems, how long they had access, how the breach occurred, and why they have not yet notified affected individuals.

30. Defendant has done little to remedy its Data Breach. Defendant has offered victims credit monitoring and identity related services. However, such services are wholly insufficient to compensate Plaintiff and Class members for the injuries that Defendant inflicted upon them.

31. Because of Defendant’s Data Breach, the PII/PHI of Plaintiff and Class members was placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiff and Class members.

32. Cybercriminals need not harvest a person’s Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff’s and the Class’s Private Information. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create “Fullz” packages, which can then be used to commit fraudulent account activity on Plaintiff’s and the Class’s financial accounts.

33. And as the Harvard Business Review notes, such “[c]ybercriminals frequently use the Dark Web—a hub of criminal and illicit activity—to sell data from companies that they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking.”<sup>7</sup>

34. Thus, on information and belief, Plaintiff’s and the Class’s stolen PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

***Plaintiff’s Experiences and Injuries***

35. Plaintiff Michael Garside is a former patient of Defendant having received services from Defendant in 2022.

36. Thus, on information and belief Defendant obtained and maintained Plaintiff’s PII/PHI.

37. As a result, Plaintiff was injured by Defendant’s Data Breach.

---

<sup>7</sup> Brenda R. Sharton, *Your Company’s Data Is for Sale on the Dark Web. Should You Buy It Back?*, HARVARD BUS. REV. (Jan. 4, 2023) <https://hbr.org/2023/01/your-companys-data-is-for-sale-on-the-dark-web-should-you-buy-it-back>.



38. As a condition of receiving services with Defendant, Plaintiff provided Defendant with his PII/PHI and allowed them to maintain his PII/PHI. Defendant used that PII/PHI to facilitate its services.

39. Plaintiff trusted the company would use reasonable measures to protect his PII/PHI according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's PII/PHI and has a continuing legal duty and obligation to protect that PII/PHI from unauthorized access and disclosure.

40. Plaintiff reasonably understood that a portion of the funds he paid for services would be used to pay for adequate cybersecurity and protection of PII/PHI.

41. Thus, on information and belief, Plaintiff's PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

42. Through its Data Breach, Defendant compromised Plaintiff's PII/PHI.

43. Plaintiff has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft and signing up for credit monitoring services.

44. Plaintiff fears for the security of his PII/PHI and worries about what information was exposed in the Data Breach.

45. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

46. Plaintiff suffered actual injury from the exposure and theft of his PII/PHI—which violates his rights to privacy.

47. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and medical identity theft—all because Defendant’s Data Breach placed Plaintiff’s PII/PHI right in the hands of criminals.

48. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate his injuries.

49. Today, Plaintiff has a continuing interest in ensuring that his PII/PHI—which, upon information and belief, remains backed up in Defendant’s possession—is protected and safeguarded from additional breaches.

***Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft***

50. Because of Defendant’s failure to prevent the Data Breach, Plaintiff and Class members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

- a. loss of the opportunity to control how their PII/PHI is used;
- b. diminution in value of their PII/PHI;
- c. compromise and continuing publication of their PII/PHI;
- d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;
- e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;
- f. delay in receipt of tax refund monies;
- g. unauthorized use of their stolen PII/PHI; and

h. continued risk to their PII/PHI—which remains in Defendant’s possession—and is thus at risk for future breaches so long as Defendant fails to take appropriate measures to protect the PII/PHI.

51. Stolen PII/PHI is one of the most valuable commodities on the criminal information black market.

52. According to the National Association of Healthcare Access Management, “[p]ersonal medical data is said to be more than ten times as valuable as credit card information. PHI has such a high value because it contains highly sensitive information, such as social security numbers, birth dates, addresses, credit card numbers, telephone numbers and medical conditions. This data is incredibly valuable on the black market because, unlike a stolen credit card that can be easily canceled, most people are unaware that their medical information has been stolen.”<sup>8</sup>

53. According to Advent Health University, when an electronic health record “lands in the hands of nefarious persons the results can range from fraud to identity theft to extortion. In fact, these records provide such valuable information that hackers can sell a single stolen medical record for up to \$1,000.”<sup>9</sup>

54. Because of the value of its collected and stored data, the medical industry has experienced disproportionately higher numbers of data theft events than other industries.

55. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase Private Information on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach

---

<sup>8</sup> <https://www.naham.org/page/ConnectionsThe-Value-of-Personal-Medical-Information#:~:text=Personal%20medical%20data%20is%20said,telephone%20numbers%20and%20medical%20conditions>, (last visited May 19, 2025).

<sup>9</sup> <https://www.ahu.edu/blog/data-security-in-healthcare> (last visited May 19, 2025).

victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

56. According to an article in the HIPAA Journal posted on October 14, 2022, cybercriminals hack into medical practices for their “highly prized” medical records. “[T]he number of data breaches reported by HIPAA-regulated entities continues to increase every year. 2021 saw 714 data breaches of 500 or more records reported to the [HHS’ Office for Civil Rights] OCR – an 11% increase from the previous year. Almost three-quarters of those breaches were classified as hacking/IT incidents.”<sup>10</sup>

57. Healthcare organizations are easy targets because “even relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly detailed, including demographic data, Social Security numbers, financial information, health insurance information, and medical and clinical data, and that information can be easily monetized.”<sup>11</sup>

58. The HIPAA Journal article goes on to explain that patient records, like those stolen from Defendant, are “often processed and packaged with other illegally obtained data to create full record sets (the previously mentioned Fullz package) that contain extensive information on individuals, often in intimate detail.” The record sets are then sold on dark web sites to other criminals and “allows an identity kit to be created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities.”<sup>12</sup>

---

<sup>10</sup> <https://www.hipaajournal.com/why-do-criminals-target-medical-records/> (last visited May 19, 2025).

<sup>11</sup> *Id.*

<sup>12</sup> *Id.*

59. Data breaches such as the one experienced by Defendant have become so notorious that the Federal Bureau of Investigation (“FBI”) and U.S. Secret Service have issued a warning to potential targets so they are aware of, can prepare for, and hopefully can ward off a potential attack.

60. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.<sup>13</sup>

61. These significant increases in attacks to companies, particularly those in the healthcare industry, and attendant risk of future attacks, is widely known to the public and to anyone in that industry, including Defendant.

62. A study by Experian found that the average total cost of medical identity theft is “nearly \$13,500” per incident, and that many victims were forced to pay out-of-pocket costs for fraudulent medical care.<sup>14</sup> Victims of healthcare data breaches often find themselves “being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores.”<sup>15</sup>

63. Moreover, there may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

---

<sup>13</sup> <https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack> (last visited May 19, 2025).

<sup>14</sup> <https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/> (last visited May 19, 2025).

<sup>15</sup> *Id.*

64. It is incorrect to assume that reimbursing a victim for a financial loss due to fraud makes that individual whole again. Similar to the GAO's study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had personal information used for fraudulent purposes, about a third (32%) spent a month or more resolving problems."<sup>16</sup> In fact, the BJS reported, "resolving the problems caused by identity theft [could] take more than a year for some victims."<sup>17</sup>

65. Further, once a patient's medical information is in the hands of thieves, they have access to the individual's health insurance and may use it to obtain free medical care, which can "ruin credit and take months, or even years, to resolve."<sup>18</sup>

66. As the fraudulent activity resulting from the Data Breach may not come to light for years, Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

***Defendant Knew—Or Should Have Known—of the Risk of a Data Breach***

67. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years.

68. In 2021, a record 1,862 data breaches occurred, exposing approximately 293,927,708 sensitive records—a 68% increase from 2020.<sup>19</sup>

69. Indeed, cyberattacks have become so notorious that the Federal Bureau of

---

<sup>16</sup> <https://bjs.ojp.gov/content/pub/pdf/vit14.pdf> (last visited May 19, 2025).

<sup>17</sup> *Id.*

<sup>18</sup> <https://www.naham.org/page/ConnectionsThe-Value-of-Personal-Medical-Information#:~:text=Personal%20medical%20data%20is%20said,telephone%20numbers%20and%20medical%20conditions> (last visited May 19, 2025).

<sup>19</sup> See 2021 Data Breach Annual Report, IDENTITY THEFT RESOURCE CENTER (Jan. 2022) <https://notified.idtheftcenter.org/s/>.

Investigation (“FBI”) and U.S. Secret Service issue warnings to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, “[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly.”<sup>20</sup>

70. Defendant’s Data Breach follows a number of high-profile data breaches of US healthcare providers. This includes the Change Healthcare ransomware attack in February, 2024, which has led to more than 100 million Americans’ personal data being breached and a ransomware attack on Ascension in May in resulted in 5.6 million individuals having their sensitive personal, medical and financial information breached.<sup>21</sup>

71. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant’s industry, including Defendant.

#### ***Defendant Failed to Follow FTC Guidelines***

72. According to the Federal Trade Commission (“FTC”), the need for data security should be factored into all business decision-making. Thus, the FTC issued numerous guidelines identifying best data security practices that businesses—like Defendant—should use to protect against unlawful data exposure.

---

<sup>20</sup> Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), <https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware>.

<sup>21</sup> <https://www.infosecurity-magazine.com/news/Defendant-breach-patient-data/> (last visited May 19, 2025).

73. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for what data security principles and practices businesses must use.<sup>22</sup> The FTC declared that, *inter alia*, businesses must:

- a. protect the personal customer information that they keep;
- b. properly dispose of personal information that is no longer needed;
- c. encrypt information stored on computer networks;
- d. understand their network's vulnerabilities; and
- e. implement policies to correct security problems.

74. The guidelines also recommend that businesses watch for the transmission of large amounts of data out of the system—and then have a response plan ready for such a breach.

75. Furthermore, the FTC explains that companies must:

- a. not maintain information longer than is needed to authorize a transaction;
- b. limit access to sensitive data;
- c. require complex passwords to be used on networks;
- d. use industry-tested methods for security;
- e. monitor for suspicious activity on the network; and
- f. verify that third-party service providers use reasonable security measures.

76. The FTC brings enforcement actions against businesses for failing to protect customer data adequately and reasonably. Thus, the FTC treats the failure—to use reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15

---

<sup>22</sup> *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016) [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136\\_proteting-personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf).



U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

77. In short, Defendant's failure to use reasonable and appropriate measures to protect against unauthorized access to its current and former patients' data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

***Defendant Failed to Follow Industry Standards***

78. Several best practices have been identified that—at a *minimum*—should be implemented by businesses like Defendant. These industry standards include: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

79. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

80. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR.DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04).

81. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

***Defendant Violated HIPAA***

82. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.<sup>23</sup>

83. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PHI and PHI is properly maintained.<sup>24</sup>

84. The Data Breach itself resulted from a combination of inadequacies showing Defendant failed to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

- a. failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

---

<sup>23</sup> HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

<sup>24</sup> See 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

- b. failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);
- c. failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);
- d. failing to ensure compliance with HIPAA security standards by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);
- e. failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);
- f. failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);
- g. failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);
- h. failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

- i. failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

85. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations.

### **CLASS ACTION ALLEGATIONS**

86. Plaintiff brings this class action under Missouri Court Rule of Civil Procedure 52.08, individually and on behalf of all members of the following class:

All individuals residing in the United States whose PII/PHI was compromised in the Data Breach including all those individuals who received notice of the breach.

87. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

88. Plaintiff reserves the right to amend the class definition.

89. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

90. Ascertainability. All members of the proposed Class are readily ascertainable from information in Defendant's custody and control.

91. Numerosity. The Class members are so numerous that joinder of all Class members is impracticable. Upon information and belief, the proposed Class includes at least thousands of members.

92. Typicality. Plaintiff's claims are typical of Class members' claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

93. Adequacy. Plaintiff will fairly and adequately protect the proposed Class's common interests. His interests do not conflict with Class members' interests. And Plaintiff has retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

94. Commonality and Predominance. Plaintiff's and the Class's claims raise predominantly common fact and legal questions—which predominate over any questions affecting individual Class members—for which a class wide proceeding can answer for all Class members. In fact, a class wide proceeding is necessary to answer the following questions:

- a. if Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII/PHI;
- b. if Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- c. if Defendant were negligent in maintaining, protecting, and securing PII/PHI;
- d. if Defendant breached contract promises to safeguard Plaintiff and the Class's PII/PHI;
- e. if Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;
- f. if Defendant's Breach Notice was reasonable;

- g. if the Data Breach caused Plaintiff and the Class injuries;
- h. what the proper damages measure is; and
- i. if Plaintiff and the Class are entitled to damages, treble damages, and or injunctive relief.

95. Superiority. A class action will provide substantial benefits and is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that individual litigation against Defendant would require. Thus, it would be practically impossible for Class members, on an individual basis, to obtain effective redress for their injuries. Not only would individualized litigation increase the delay and expense to all parties and the courts, but individualized litigation would also create the danger of inconsistent or contradictory judgments arising from the same set of facts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale, provides comprehensive supervision by a single court, and presents no unusual management difficulties.

**FIRST CAUSE OF ACTION**  
**Negligence**  
**(On Behalf of Plaintiff and the Class)**

96. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

97. Plaintiff and the Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their PII, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

98. Defendant owed a duty of care to Plaintiff and Class Members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry

standards for data security—would compromise their PII in a data breach. And here, that foreseeable danger came to pass.

99. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if their PII was wrongfully disclosed.

100. Defendant owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiff and Class Members' PII.

101. Defendant owed—to Plaintiff and Class Members—at least the following duties to:

- a. exercise reasonable care in handling and using the PII in its care and custody;
- b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;
- c. promptly detect attempts at unauthorized access;
- d. notify Plaintiff and Class Members within a reasonable timeframe of any breach to the security of their PII.

102. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiff and Class Members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

103. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII it was no longer required to retain under applicable regulations.

104. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

105. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a necessary part of obtaining services from Defendant.

106. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant hold vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII — whether by malware or otherwise.

107. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and Class Members' and the importance of exercising reasonable care in handling it.

108. Defendant improperly and inadequately safeguarded the PII of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

109. Defendant breached these duties as evidenced by the Data Breach.

110. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class Members' PII by:

- a. disclosing and providing access to this information to third parties and



- b. failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

111. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiff and Class Members which actually and proximately caused the Data Breach and Plaintiff and Class Members' injury.

112. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and Class Members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff and Class Members' injuries-in-fact.

113. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

114. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class Members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

115. And, on information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

116. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted

from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

**SECOND CAUSE OF ACTION**  
**Negligence *per se***  
**(On Behalf of Plaintiff and the Class)**

117. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

118. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

119. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the PII entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff and the Class Members' sensitive PII.

120. Defendant breached its respective duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII.

121. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

122. Similarly, under HIPAA, Defendant had a duty to follow HIPAA standards for privacy and security practices—as to protect Plaintiff's and Class members' PII/PHI.

123. Defendant violated its duty under HIPAA by failing to use reasonable measures to protect its PII/PHI and by not complying with applicable regulations detailed *supra*. Here too, Defendant's conduct was particularly unreasonable given the nature and amount of PII/PHI that Defendant collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

124. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

125. But for Defendant's wrongful and negligent breach of its duties owed, Plaintiff and Class Members would not have been injured.

126. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

127. Defendant's various violations and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

128. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

**THIRD CAUSE OF ACTION**  
**Breach of Implied Contract**  
**(On Behalf of Plaintiff and the Class)**

129. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

130. Plaintiff and Class members were required to provide their PII/PHI to Defendant as a condition of receiving services provided by Defendant. Plaintiff and Class members provided their PII/PHI to Defendant in exchange for Defendant's services.

131. Plaintiff and Class members reasonably understood that a portion of the funds they paid Defendant would be used to pay for adequate cybersecurity measures.

132. Plaintiff and Class members reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII/PHI that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

133. Plaintiff and the Class members accepted Defendant's offers by disclosing their PII/PHI to Defendant in exchange for services.

134. In turn, and through internal policies, Defendant agreed to protect and not disclose the PII/PHI to unauthorized persons.

135. In its Privacy Policy, Defendant represented that they had a legal duty to protect Plaintiff's and Class Member's PII/PHI.

136. Implicit in the parties' agreement was that Defendant would provide Plaintiff and Class members with prompt and adequate notice of all unauthorized access and/or theft of their PII/PHI.

137. After all, Plaintiff and Class members would not have entrusted their PII/PHI to Defendant in the absence of such an agreement with Defendant.

138. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

139. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair

dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

140. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

141. Defendant materially breached the contracts it entered with Plaintiff and Class members by:

- a. failing to safeguard their information;
- b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.
- c. failing to comply with industry standards;
- d. failing to comply with the legal obligations necessarily incorporated into the agreements; and
- e. failing to ensure the confidentiality and integrity of the electronic PII/PHI that Defendant created, received, maintained, and transmitted.

142. In these and other ways, Defendant violated its duty of good faith and fair dealing.

143. Defendant's material breaches were the direct and proximate cause of Plaintiff's and Class members' injuries (as detailed *supra*).

144. And, on information and belief, Plaintiff's PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

145. Plaintiff and Class members performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

**FOURTH CAUSE OF ACTION**  
**Invasion of Privacy**  
**(On Behalf of Plaintiff and the Class)**

146. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

147. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII/PHI and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

148. Defendant owed a duty to its current and former patients, including Plaintiff and the Class, to keep this information confidential.

149. The unauthorized acquisition (i.e., theft) by a third party of Plaintiff and Class members' PII/PHI is highly offensive to a reasonable person.

150. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

151. The Data Breach constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

152. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

153. Defendant acted with a knowing state of mind when it failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

154. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

155. As a proximate result of Defendant's acts and omissions, the private and sensitive PII/PHI of Plaintiff and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages (as detailed *supra*).

156. And, on information and belief, Plaintiff's PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

157. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII/PHI are still maintained by Defendant with their inadequate cybersecurity system and policies.

158. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII/PHI of Plaintiff and the Class.

159. In addition to injunctive relief, Plaintiff, on behalf of himself and the other Class members, also seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

**FIFTH CAUSE OF ACTION**  
**Unjust Enrichment**  
**(On Behalf of Plaintiff and the Class)**

160. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

161. This claim is pleaded in the alternative to the breach of implied contract claim.

162. Plaintiff and Class members conferred a benefit upon Defendant. After all, Defendant benefitted from using their PII/PHI to provide services and benefitted from the payment provided in exchange for services.

163. Defendant appreciated or had knowledge of the benefits it received from Plaintiff and Class members.

164. Plaintiff and Class members reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII/PHI that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

165. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class members' PII/PHI.

166. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class members by utilizing cheaper, ineffective security measures. Plaintiff and Class members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

167. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and Class members' payment because Defendant failed to adequately protect their PII/PHI.

168. Plaintiff and Class members have no adequate remedy at law.



169. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiff and Class members—all unlawful or inequitable proceeds that it received because of its misconduct.

**SIXTH CAUSE OF ACTION**  
**Breach of Fiduciary Duty**  
**(On Behalf of Plaintiff and the Class)**

170. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

171. Given the relationship between Defendant and Plaintiff and Class members, where Defendant became guardian of Plaintiff's and Class members' PII/PHI, Defendant became a fiduciary by its undertaking and guardianship of the PII/PHI, to act primarily for Plaintiff and Class members, (1) for the safeguarding of Plaintiff and Class members' PII/PHI; (2) to timely notify Plaintiff and Class members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

172. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of Defendant's relationship with them—especially to secure their PII/PHI.

173. Because of the highly sensitive nature of the PII/PHI, Plaintiff and Class members would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII/PHI had they known the reality of Defendant's inadequate data security practices.

174. Defendant breached its fiduciary duties to Plaintiff and Class members by failing to sufficiently encrypt or otherwise protect Plaintiff's and Class members' PII/PHI.

175. Defendant also breached its fiduciary duties to Plaintiff and Class members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

176. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

### **PRAYER FOR RELIEF**

Plaintiff and Class members respectfully request judgment against Defendant and that the Court enter an order:

- A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing her counsel to represent the Class;
- B. Awarding declaratory and other equitable relief as necessary to protect the interests of Plaintiff and the Class;
- C. Awarding injunctive relief as necessary to protect the interests of Plaintiff and the Class;
- D. Enjoining Defendant from further unfair and/or deceptive practices;
- E. Awarding Plaintiff and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;
- F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;
- G. Awarding attorneys' fees and costs, as allowed by law;
- H. Awarding prejudgment and post-judgment interest, as provided by law;
- I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and
- J. Granting other relief that this Court finds appropriate.

### DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial for all claims so triable.

Date: May 19, 2025

Respectfully submitted,

/s/ John F. Garvey

John F. Garvey #35879

Colleen Garvey #72809

Ellen A. Thomas, #73043

STRANCH, JENNINGS & GARVEY, PLLC

701 Market Street

Peabody Plaza, Suite 1510

St. Louis, Missouri 63101

(314) 390-6750

[jgarvey@stranchlaw.com](mailto:jgarvey@stranchlaw.com)

[cgarvey@stranchlaw.com](mailto:cgarvey@stranchlaw.com)

[ethomas@stranchlaw.com](mailto:ethomas@stranchlaw.com)

Raina Borrelli\*

**STRAUSS BORRELLI, PLLC**

980 N. Michigan Avenue, Suite 1610

Chicago, Illinois 60611

T: (872) 263-1100

F: (872) 263-1109

[raina@straussborrelli.com](mailto:raina@straussborrelli.com)

*\*Pro hac vice forthcoming*

*Attorneys for Plaintiff and Proposed Class*

In the  
**CIRCUIT COURT**  
Of St. Louis County, Missouri



For File Stamp Only

Michael Garside, on behalf of himself and all others similarly situated  
Plaintiff/Petitioner

May 19, 2025  
Date

Case Number

vs.

American Multispecialty Group, Inc.  
Defendant/Respondent

Division

**REQUEST FOR APPOINTMENT OF PROCESS SERVER**

Comes now Plaintiff, pursuant  
Requesting Party

to Local Rule 28, and at his/her/its own risk requests the appointment of the Circuit Clerk of  
H&H Investigations, 432 Hazelgreen, St. Louis, MO 63119 (314) 225-8114  
Name of Process Server Address Telephone

Name of Process Server Address or in the Alternative Telephone

Name of Process Server Address or in the Alternative Telephone

Natural person(s) of lawful age to serve the summons and petition in this cause on the below  
named parties. This appointment as special process server does not include the authorization  
to carry a concealed weapon in the performance thereof.

SERVE:  
American Multispecialty Group, Inc.  
Name  
12655 Olive Blvd., Floor4  
Address  
St. Louis, MO 63141  
City/State/Zip

SERVE:  
\_\_\_\_\_  
Name  
\_\_\_\_\_  
Address  
\_\_\_\_\_  
City/State/Zip


SERVE:  
\_\_\_\_\_  
Name  
\_\_\_\_\_  
Address  
\_\_\_\_\_  
City/State/Zip

SERVE:  
\_\_\_\_\_  
Name  
\_\_\_\_\_  
Address  
\_\_\_\_\_  
City/State/Zip

Appointed as requested:  
**JOAN M. GILMER**, Circuit Clerk

By \_\_\_\_\_  
Deputy Clerk

Date

  
\_\_\_\_\_  
Signature of Attorney/Plaintiff/Petitioner  
35879  
Bar No.  
701 Market St., Ste. 1510, St. Louis, MO 63101  
Address  
(314) 390-6750  
Phone No. Fax No.

#### Local Rule 28. SPECIAL PROCESS SERVERS

(1) Any Judge may appoint a Special Process Server in writing in accordance with the law and at the risk and expense of the requesting party except no special process server shall be appointed to serve a garnishment [except as allowed by Missouri Supreme Court Rule 90.03(a)].

This appointment as Special Process Server does not include the authorization to carry a concealed weapon in the performance thereof.

(2) The Circuit Clerk may appoint a natural person other than the Sheriff to serve process in any cause in accordance with this subsection;

(A) Appointments may list more than one server as alternates.

(B) The appointment of a person other than the Sheriff to serve process shall be made at the risk and expense of the requesting party.

(C) Any person of lawful age, other than the Sheriff, appointed to serve process shall be a natural person and not a corporation or other business association.

(D) No person, other than the Sheriff, shall be appointed to serve any order, writ or other process which requires any levy, seizure, sequestration, garnishment, [except as allowed by Missouri Supreme Court Rule 90.03(a)], or other taking.

(E) Requests for appointment of a person other than the Sheriff to serve process shall be made on a "Request for Appointment of Process Server" electronic form, which may be found on the Court's Web Site,

<https://stlcourtscourts.com/forms/associate-civil/request-process-server/>

(F) This appointment as Special Process Server does not include the authorization to carry a concealed weapon in the performance thereof.

#### SERVICE RETURN

Any service by the St. Louis County Sheriff's Office shall be scanned into the courts case management system. Any service by another Sheriff or a Special Process Server or any other person authorized to serve process shall return to the attorney or party who sought service and the attorney shall file the return electronically to the Circuit Clerk.





## Summons in Civil Case

IN THE 21ST JUDICIAL CIRCUIT, ST. LOUIS COUNTY, MISSOURI

Judge or Division: JOHN ROBERT LASATER	Case Number: <b>25SL-CC05454</b>	
Plaintiff/Petitioner: MICHAEL GARSIDE	Plaintiff's/Petitioner's Attorney/Address JOHN FRANCIS GARVEY JR 701 MARKET ST SUITE 1510 ST LOUIS, MO 63101	
Defendant/Respondent: AMERICAN MULTISPECIALTY GROUP, INC. DBA: ESSE HEALTH	Court Address: ST LOUIS COUNTY COURT BUILDING 105 SOUTH CENTRAL AVENUE CLAYTON, MO 63105	
Nature of Suit: CC Breach of Contract		(Date File Stamp for Return)

The State of Missouri to: **AMERICAN MULTISPECIALTY GROUP, INC.**  
Alias:  
**DBA: ESSE HEALTH**

**12655 OLIVE BLVD., FLOOR 4**  
**ST. LOUIS, MO 63141**

You are summoned to appear before this court and to file your pleading to the petition, a copy of which is attached, and to serve a copy of your pleading upon the attorney for plaintiff/petitioner at the above address all within 30 days after receiving this summons, exclusive of the day of service. If you fail to file your pleading, judgment by default may be taken against you for the relief demanded in the petition.

### COURT SEAL OF



**ST. LOUIS COUNTY**

20-MAY-2025

Date

/S/ Adam Dockery

Clerk

### Further Information:

AD

### Officer's or Server's Return

**Note to serving officer:** Service should be returned to the court within 30 days after the date of issue.

I certify that I have served the above Summons by: (check one)

- ☐ delivering a copy of the summons and petition to the defendant/respondent.
- ☐ leaving a copy of the summons and petition at the dwelling house or usual place of abode of the defendant/respondent with \_\_\_\_\_, a person at least 18 years of age residing therein.
- ☐ (for service on a corporation) delivering a copy of the summons and petition to: \_\_\_\_\_ (name) \_\_\_\_\_ (title).
- ☐ other: \_\_\_\_\_.

Served at \_\_\_\_\_ (address)  
in \_\_\_\_\_ (County/City of St. Louis), MO, on \_\_\_\_\_ (date)  
at \_\_\_\_\_ (time).

\_\_\_\_\_  
Printed Name of Officer or Server

\_\_\_\_\_  
Signature of Officer or Server

**Must be sworn before a notary public if not served by an authorized officer.**

Subscribed and sworn to before me on \_\_\_\_\_ (date).

(Seal)

My commission expires: \_\_\_\_\_  
Date Notary Public

#### Service Fees (if applicable)

Summons	\$ _____
Non Est	\$ _____
Sheriff's Deputy Salary	
Supplemental Surcharge	\$ 10.00
Mileage	\$ _____ ( _____ miles @ \$. _____ per mile)
<b>Total</b>	<b>\$ _____</b>

A copy of the summons and petition must be served on **each** defendant/respondent. For methods of service on all classes of suits, see Supreme Court Rule 54.

## THE CIRCUIT COURT OF ST. LOUIS COUNTY, MISSOURI

Twenty First Judicial Circuit

### NOTICE OF ALTERNATIVE DISPUTE RESOLUTION SERVICES

#### **Purpose of Notice**

As a party to a lawsuit in this court, you have the right to have a judge or jury decide your case. However, most lawsuits are settled by the parties before a trial takes place. This is often true even when the parties initially believe that settlement is not possible. A settlement reduces the expense and inconvenience of litigation. It also eliminates any uncertainty about the results of a trial.

Alternative dispute resolution services and procedures are available that may help the parties settle their lawsuit faster and at less cost. Often such services are most effective in reducing costs if used early in the course of a lawsuit. Your attorney can aid you in deciding whether and when such services would be helpful in your case.

#### **Your Rights and Obligations in Court Are Not Affected By This Notice**

You may decide to use an alternative dispute resolution procedure if the other parties to your case agree to do so. In some circumstances, a judge of this court may refer your case to an alternative dispute resolution procedure described below. These procedures are not a substitute for the services of a lawyer and consultation with a lawyer is recommended. Because you are a party to a lawsuit, you have obligations and deadlines which must be followed whether you use an alternative dispute resolution procedure or not. **IF YOU HAVE BEEN SERVED WITH A PETITION, YOU MUST FILE A RESPONSE ON TIME TO AVOID THE RISK OF DEFAULT JUDGMENT, WHETHER OR NOT YOU CHOOSE TO PURSUE AN ALTERNATIVE DISPUTE RESOLUTION PROCEDURE.**

#### **Alternative Dispute Resolution Procedures**

There are several procedures designed to help parties settle lawsuits. Most of these procedures involve the services of a neutral third party, often referred to as the “neutral,” who is trained in dispute resolution and is not partial to any party. The services are provided by individuals and organizations who may charge a fee for this help. Some of the recognized alternative dispute resolutions procedures are:

**(1) Advisory Arbitration:** A procedure in which a neutral person or persons (typically one person or a panel of three persons) hears both sides and decides the case. The arbitrator’s decision is not binding and simply serves to guide the parties in trying to settle their lawsuit. An arbitration is typically less formal than a trial, is usually shorter, and may be conducted in a private setting at a time mutually agreeable to the parties. The parties, by agreement, may select the arbitrator(s) and determine the rules under which the arbitration will be conducted.



**(2) Mediation:** A process in which a neutral third party facilitates communication between the parties to promote settlement. An effective mediator may offer solutions that have not been considered by the parties or their lawyers. A mediator may not impose his or her own judgment on the issues for that of the parties.

**(3) Early Neutral Evaluation (“ENE”):** A process designed to bring the parties to the litigation and their counsel together in the early pretrial period to present case summaries before and receive a non-binding assessment from an experienced neutral evaluator. The objective is to promote early and meaningful communication concerning disputes, enabling parties to plan their cases effectively and assess realistically the relative strengths and weaknesses of their positions. While this confidential environment provides an opportunity to negotiate a resolution, immediate settlement is not the primary purpose of this process.

**(4) Mini-Trial:** A process in which each party and their counsel present their case before a selected representative for each party and a neutral third party, to define the issues and develop a basis for realistic settlement negotiations. The neutral third party may issue an advisory opinion regarding the merits of the case. The advisory opinion is not binding.

**(5) Summary Jury Trial:** A summary jury trial is a non binding, informal settlement process in which jurors hear abbreviated case presentations. A judge or neutral presides over the hearing, but there are no witnesses and the rules of evidence are relaxed. After the “trial”, the jurors retire to deliberate and then deliver an advisory verdict. The verdict then becomes the starting point for settlement negotiations among the parties.

### **Selecting an Alternative Dispute Resolution Procedure and a Neutral**

If the parties agree to use an alternative dispute resolution procedure, they must decide what type of procedure to use and the identity of the neutral. As a public service, the St. Louis County Circuit Clerk maintains a list of persons who are available to serve as neutrals. The list contains the names of individuals who have met qualifications established by the Missouri Supreme Court and have asked to be on the list. The Circuit Clerk also has Neutral Qualifications Forms on file. These forms have been submitted by the neutrals on the list and provide information on their background and expertise. They also indicate the types of alternative dispute resolution services each neutral provides.

A copy of the list may be obtained by request in person and in writing to: Circuit Clerk, Office of Dispute Resolution Services, 105 South Central Avenue, 5th Floor, Clayton, Missouri 63105. The Neutral Qualifications Forms will also be made available for inspection upon request to the Circuit Clerk.

The List and Neutral Qualification Forms are provided only as a convenience to the parties in selecting a neutral. The court cannot advise you on legal matters and can only provide you with the List and Forms. You should ask your lawyer for further information.



**OFFICE OF THE CIRCUIT CLERK**

Missouri's 21<sup>st</sup> Judicial Circuit, St. Louis County

Civil Department

105 South Central Avenue, Clayton, MO 63105

Hours: Monday through Friday 8:00 A.M. to 5:00 P.M.

Phone: 314-615-8029

SPECIAL NEEDS: If you have special needs addressed by the Americans With Disabilities Act. Please notify the Office of the Circuit Clerk at 314-615-8029. FAX 314-615-8739, email at [SLCADA@courts.mo.gov](mailto:SLCADA@courts.mo.gov), or through Relay Missouri by dialing 711 Or 800-735-2966, at least three business days in advance of the court proceeding.





**Summons in Civil Case**

IN THE 21ST JUDICIAL CIRCUIT, ST. LOUIS COUNTY, MISSOURI

Judge or Division: JOHN ROBERT LASATER	Case Number: 25SL-CC05454	(Date File Stamp for Return)
Plaintiff/Petitioner: MICHAEL GARSIDE	Plaintiff's/Petitioner's Attorney/Address JOHN FRANCIS GARVEY JR 701 MARKET ST SUITE 1510 ST LOUIS, MO 63101	
Defendant/Respondent: AMERICAN MULTISPECIALTY GROUP, INC. DBA: ESSE HEALTH	Court Address: ST LOUIS COUNTY COURT BUILDING 105 SOUTH CENTRAL AVENUE CLAYTON, MO 63105	
Nature of Suit: CC Breach of Contract		

The State of Missouri to: AMERICAN MULTISPECIALTY GROUP, INC.  
Alias:  
DBA: ESSE HEALTH

12655 OLIVE BLVD., FLOOR 4  
ST. LOUIS, MO 63141

You are summoned to appear before this court and to file your pleading to the petition, a copy of which is attached, and to serve a copy of your pleading upon the attorney for plaintiff/petitioner at the above address all within 30 days after receiving this summons, exclusive of the day of service. If you fail to file your pleading, judgment by default may be taken against you for the relief demanded in the petition.

**COURT SEAL OF**



**ST. LOUIS COUNTY**

20-MAY-2025  
Date

/S/ Adam Dockery  
Clerk

Further Information:  
AD



Case Number: 25SL-CC05454

Officer's or Server's Return

**Note to serving officer:** Service should be returned to the court within 30 days after the date of issue.

I certify that I have served the above Summons by: (check one)

- ☐ delivering a copy of the summons and petition to the defendant/respondent.
- ☐ leaving a copy of the summons and petition at the dwelling house or usual place of abode of the defendant/respondent with \_\_\_\_\_, a person at least 18 years of age residing therein.

☒ (for service on a corporation) delivering a copy of the summons and petition to:  
\_\_\_\_\_ (name) \_\_\_\_\_ (title).

☐ other: \_\_\_\_\_

Served at 12655 Olive Blvd St. Louis Mo 63141 (address)  
in St. Louis (County/City of St. Louis), MO, on 5/23/25 (date)  
at 11:37am (time).

Joseph Delan Special Process Server # 722  
Printed Name of Officer or Server

[Signature] SPS # 722  
Signature of Officer or Server

Diane L McKay  
Notary Public, Notary Seal  
State of Missouri  
St. Louis County  
My Commission Expires 11/11/2029  
Commission # 13470566

**Must be sworn before a notary public if not served by an authorized officer.**

Subscribed and sworn to before me on 5/27/25 (date).

My commission expires: 4/11/29 Date  
[Signature] Notary Public

**Service Fees (if applicable)**

Summons	\$ _____
Non Est	\$ _____
Sheriff's Deputy Salary	
Supplemental Surcharge	\$ <u>10.00</u>
Mileage	\$ _____ ( _____ miles @ \$ _____ per mile)
Total	\$ _____

A copy of the summons and petition must be served on **each** defendant/respondent. For methods of service on all classes of suits, see Supreme Court Rule 54.